The City of
Provo, Utah

Provo

January 19, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

I was thrillied to read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As the Telecommunications Manager for the City of Provo, a Utah community of 120,000, I am encouraged by the proposed rulemaking. Even though we have taken each and every protective step recommended by the IXC's and CPE vendors, we still experienced toll fraud. I have sadly learned that it is impossible to secure any system from toll fraud.

I firmly believe that PBX owners should not be responsible for 100% of the toll fraud, since we don't have 100% control. Our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided by IXCs, LECs, and CPEs. The law should reflect that.

It is preposterous to think that the IXCs, LECs and CPEs have absolutely no legal obligations to even warn customers. It is galling to know, that these service and equipment providers consistently receive payment for the fraudulent calls made through equipment belonging to helpless PBX owners, and in many cases -- full payment. Where is their incentive to stop fraud? They appear to be much more concerned with limiting their liability.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs sell equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later. It is vital that the FCC establish a standard for caller identification and require the IXCs and LECs to pass this information. This would simplify both the identification and prosecution of hackers.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to

Division of Facility Services

351 West Center
P.O. Box 1849
Provo, Utah 84603-1849

801-379-6630
FAX: 801-379-6690

preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, toll fraud, when it did occur, could be limited to hours instead of days. The FCC should also consider requiring the LECs to offer monitoring services similar to the IXCs, as hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and education services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause. The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when hackers state, they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the $5 billion problem it is today. We must develop legislation that both clearly defines and penalizes this criminal activity and gives law enforcement the means to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am sure that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

Alan L DeWitt

Alan L. DeWitt
Provo City Corporation
Facility Services Division